Digital Watermarking: A survey on image watermarking in Frequency Domain using Genetic Algorithm

Vagesh Porwal[1], Siddharth Gupta[2]

1Department of Computer Science and Engineering, Galgotias University Greater Noida, Uttar Pradesh 203208, India

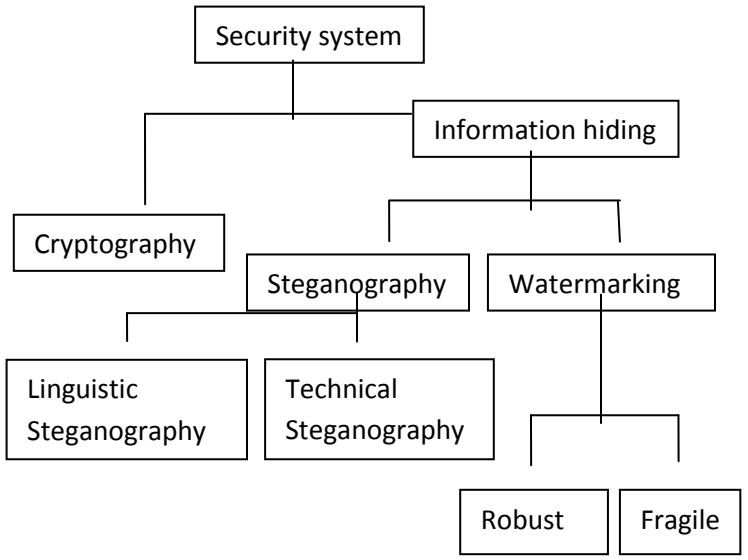
2Department of Computer Science and Engineering, Galgotias University Greater Noida, Uttar Pradesh 203208, India

Abstract

As the technology grows, its effect on our daily life becomes more and more penetrable. The same phenomenon is applied in the field of Digital image processing. As the caliber of images, audios and videos going heighten, the undesirable techniques are also applied to slip, falsify those. Hence the work of watermarking comes into effect. The watermarking technique used to avoid illegal copying of the work by embedding the digital signature or copyright image. Watermarking embeds information in the original image which is indiscernible to the human visual system. The objective of robust watermarking is to maintain the quality of an image, audio and video without affecting its originality. The work furnished in this paper is an effort to provide a survey on the latest technologies that are employed in watermarking technique.

I. Introduction

For a secure communication over the network to sustain the originality of the data, three information hiding techniques stegnography, cryptography and watermarking are tested over time and widely used to hide the original image. These three are interlinked within a security system.



The paper is organized as follows. Section II contains the types of security system. Section III contains the types of watermark and watermarking scheme. Section IV contains impact of Genetic Algorithm in watermarking and finally section V states the conclusion.

II. Security Systems

Cryptography

Cryptography is the field of mathematics that associates to the aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication.

Goals of Cryptography

1. **Confidentiality:**It is a service used to keep the content of information from all but those authorized to have it. There are numerous approaches to providing confidentiality ranging from physical protection to mathematical algorithm which deliver data unintelligible.
2. **Data integrity:**A service which addresses the unauthorized alteration of data. Data integrity can be assured by manipulating the unauthorized parties.
3. **Authentication:**A service related to recognition. This function is employed on both the entities and the information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time of origin etc.
4. **Non repudiation:** It is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying then certain actions are taken to resolve the situation.

Cryptographic systems are generally classified along three independent dimensions [25].

1. **Methodology for transforming plain text to cipher text**

   Encryption algorithms are grounded on two general principles, substitution method where each element in the plain text is mapped into another element, and transposition where elements in the plain text are rearranged.

2. **Methodology for number of keys used**

   There are some criterion [26] which is used with cryptography such as secret key, public key, digital signature and hash function.

Secret key (symmetric): It is employed for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver uses the same key to decrypt the message and recover the plain text. Secret key cryptography is also called as symmetric encryption because a single key is used for both encryption and decryption.

Public key: It is an asymmetric cryptography in which a pair of keys is used to encrypt a decrypt message so that it arrives securely. This method is practicable where two parties could engage in a secure communication over an insecure communications channel without having to share a secret key.

Digital signature: It is a cryptographic primitive which is fundamental in authentication, authorization and repudiation. The purpose of digital signature is to provide a means for an entity to bind its identity to a piece of information.

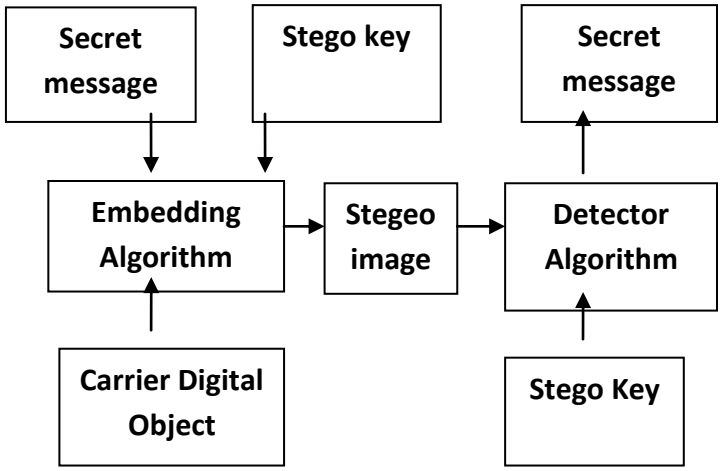
Hash function: It is a one way encryption cryptographic hash functions are mostly used for digital signatures. The hash code can be attached to the original file enabling the users to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code.

3. **Methodology for processing plain text**

   A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher.

Steganography

The word steganography comes from the Greek word ***steganos.*** Steganography is related to literally or covered writing. The objective of steganography is to communicate securely in a completely undetectable manner and to avoid drawing intuition to the transmission of a hidden data [26]. Digital images, videos, sound files and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide the secret messages. The steganographic model composed of Carriers, Message, Embedding algorithm and Stego key.
Steganography can be affected by capacity, security and robustness. The amount of information that can be hidden in the cover medium is the ***Capacity***of the medium. ***Security*** relates to an eavesdropper's inability to detect hidden information and ***Robustness***is the amount of modification that the stego medium can resist before an antagonist can destroy the hidden information.



The model of Steganography

Digital Watermarking

Fundamentally watermarking can be defined as "the process of engrafting a watermark in a multimedia object". The watermark technique divulges the ownership of the multimedia object. The basic rationalities of embedding watermark are copyright protection, content authentication, temper detection etc. visible and invisible watermarks can be embedded in the multimedia object.

Requirements of Digital Watermarking

Digital watermarking has three main requirements. They are transparency, robustness and capacity.

A. Transparency or Fidelity

Transparency explicates that the quality of the image is not compromised after the watermark is applied on it. Cox et al. (2002) define transparency or fidelity as "perceptual similarity between the original and the watermarked versions of the cover work". Transparency ascertains that there should not be any visible distortions in the image after watermarking is applied to it because it scales down the commercial value of the image.

B. Robustness

Cox et al. (2002) defines robustness as "ability to detect the watermark after common signal processing operations". A watermarked image is intentionally and unintentionally removed by a simple image processing like contrast or brightness enhancement (unintentionally) and compression, compression, filtering (intentionally). Stirmark, a benchmark to test robustness of watermarking algorithm, categorizes the attacks as

1. Attack that bump off the synchronization between embedder and the detector.
2. Attack that try to remove watermark totally.
3. Cryptographic attacks
4. Protocol attacks

C. Capacity or Data payload

"The number of bits a watermark encodes within a unit of time or work" defines the capacity or data payload cox et al. (2002). This property manages the amount of data that should embedded as a watermark for successful detection during extraction. Watermark should contain optimal information to represent the uniqueness of the image.

Watermarks and Watermark Detection

The main types of watermark that can be embedded within an image: -

A. Pseudo – Random Gaussian Sequence

A Gaussian sequence watermark is a chronological sequence of numbers comprising 1 and -1 which contains compeer 1's and -1's. This sequence is represented as a watermark with zero or one variation. A correlation measurement is used for the object detection in watermarking.

B. Binary Image or Grey Scale Image Watermark

This approach uses a logo image rather than a pseudo-random Gaussian sequence to embed substantive data by employing various watermarking techniques.

For the spotting of the watermark, a set aside decoder has to be designed based on the type of watermark embedded.
A hypothetical testing is to be exercised for the detection of the presence of watermark in a Pseudo-Random Gaussian Sequence. **W** is the original and **W'** is the extracted, watermark bit sequence respectively. BER (Bit Error Rate) is calculated to detect the presence of watermark. Zero value of BER, show the presence of watermark and if BER is one then there is no watermark. BER is calculated as follows

$$D = \begin{cases} 1, & \text{if } W_i \neq W_i' \\ 0, & \text{if } W_i = W_i' \end{cases}$$

$$BER(W, W') = \frac{\sum D}{N}$$

In Binary Image Watermarking, Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two metric functions used to compare the original image and the watermarked image in Binary Image Watermarking. It uses standard criteria as

$$MSE = \frac{\sum_{X=0}^{M-1} \sum_{y=0}^{N-1} (I(x,y) - I'(x,y))^2}{M \times N}$$

And

$$PSNR = 20 \times \log_{10} \frac{255}{Sqrt(MSE)}$$

III. Watermarking Survey

The digital watermarking is comprised of two processing domain, **the Spatial Domain and the Frequency Domain**.

Initially, most of the work has been done on the spatial domain. In Spatial domain image processing, the pixels of an image are directly manipulated. In spatial domain watermark can be embedded into a host image by substituting the less significant bits of some pixels [27], changing the paired pixels [28], and coding by textured blocks [29].

Algorithm for Spatial domain as

1. Obtain pixels from the host image

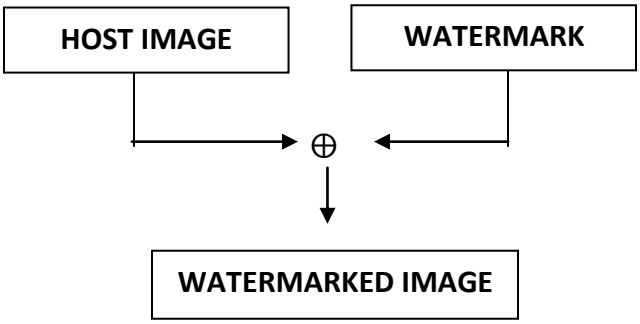
$H = \{h(I,j),\ 0 \le I, j < N\},\ h(I,j) \{0, 1, 2\ldots\ldots 2^L-1\}$

2. Obtain pixels from watermark $W = \{W(I,j),\ 0 \le I, j < M\}$

3. Substitute the pixels of the watermark into the LSB pixels of the image

   $H^* = \{h^*(I, j) = h(I,j) \oplus w(I,j),\ 0 \le I, j < N\}$,

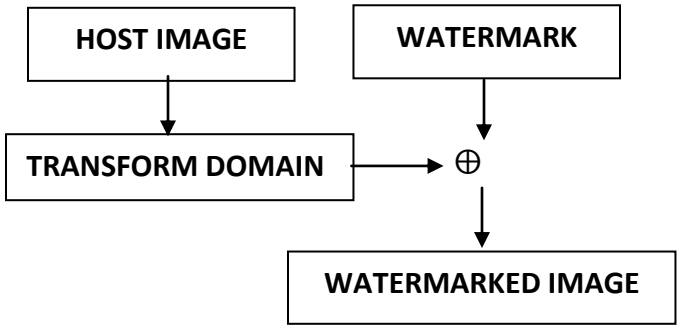
   $H^*(I,j) \in \{0, 1, 2\ldots\ldots 2^L-1\}\{0, 1, 2\ldots\ldots 2^L-1\}$



Block diagram of spatial water marking

However, the spatial domain has some retreat, these techniques are not resistant to cropping and they have low bit capacity.

The Frequency domain techniques have the capacity to embed more bits of watermark. The various approaches such as JPEG- based[30], Spread Spectrum[32, 33] and Content based approach[34] are used in the Frequency domain. Several different reversible transform such as Discrete Cosine Transform (DCT), Discrete Wavelet transform (DWT), Discrete Fourier Transform (DFT) or Singular Value Decomposition (SVD) can be used in frequency domain. In frequency domain the watermark is embedded into the coefficients of a transformed Host image. Choosing the best location for embedding watermark in the frequency domain to avoid distortion is the important consideration [35].



Block diagram of frequency domain

In this paper we attempt to elaborate the features of SVD, DCT, and DWT.

Singular Value Decomposition (SVD)

It is a method of data diminution. SVD is applied to mid-level image processing, especially to the area of image compression and recognition. Singular value decomposition is the optimal matrix decomposition in a least square sense that it packs the maximum signal energy into as few coefficients as possible [36,37].SVD is a stable and effective method to split the system into a set of linearly dependent components, and own energy contribution [36, 37].SVD is a numerical technique used to diagonalize matrices numerical analysis [38,39].SVD has the ability to manipulate the image in two distinctive subspaces and noise subspaces.

SVD image properties

Singular Value Decomposition is a robust and reliable orthogonal matrix decomposition method. This technique is more adaptive in signal processing area, due to its conceptual and stability reasons. SVD composed of various advantageous properties such as; its maximum energy packing, solving of least square problem, computing pseudo inverse of a matrix and multivariate analysis [36, 37]. Digital images are often represented by low rank matrices and, therefore are able to be described by the sum of a relatively small set of eigen images. This concept raises the manipulation of the signal as two distinct subspaces [38, 39]. Some idea will be provided and verified in the following sections. For an accomplished review, first, the SVD related theorems are summarized and then the practical properties are surveyed.

SVD Subspace:SVD is formed from two orthogonal dominant and subdominant subspaces. This corresponds to partition the m-directional vector space into dominant and subdominant subspaces [36, 40]. This property of SVD is utilized in noise filtering and watermarking.

SVD architecture: Singular value (SV) specifies that the luminance of an image layer and the corresponding singular vectors (sc) specify the geometry of the image layer, where SVD decomposition of an image is performed. The largest object components in an image found using the SVD generally correspond to eigen images associated with the largest singular values, while image noise corresponds to eigen images associated with the SVs [38, 39].

PCA versus SVD: Principal Component Analysis (PCA) used to compute the dominant vectors representing a given data set and provides an optimal basis for minimum mean squared reconstruction of the given data.
The foundation of PCA is the calculation of the SVD of the data matrix. Singular Value Decomposition closely related to to the standard eigen values, eigenvactors or spectral decomposition of a square matrix X, into VLV', where V is orthogonal and L are diagonal [38, 39].

SVD Multiresolution: Singular value decomposition is practicable to obtain a statistical characterization of an image at several resolutions. For obtaining optimal sub rank approximations, SVD decomposes a matrix into orthogonal components. In multiresolution SVD, following characteristics of an image may be measured such as isotropy, spercity of principal components, self-similarity under scaling, and resolution of the mean squared error into meaningful components.

SVD Oriented Energy: Both the rank of the problem and signal space orientation can be determined, in energy oriented analysis of SVD. Singular value decomposition is a stable and effective method to split the system into a set of linearly independent components, each of these bearing its own energy contribution. The oriented energy concept is an effective tool to separate signal from different sources, or to select signal subspace of maximal signal activity and integrity.

Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) is used for image comparison in frequency domain. Well comprise between information packing ability and computational complexity is the key feature of DCT. Discrete cosine transform is more robust to various image processing technique like filtering,

bluing brightness and contrast adjustment etc. although these are decrepit to geometric attacks like rotation, scaling, cropping etc.

In Discrete Cosine Transform an image can be broken down into three different frequency bands High frequency components block (F_H), Middle frequency components block (F_M) and Low frequency components block (F_L). The watermark is embedded into the Middle frequency band (F_M).

In their work DeeptiAgrawal [8], proposed a technique based on DCT and image segmentation. They uses expectation maximization segmentation algorithm and a zigzag recording is applied to each block of each segment. Then a pseudorandom sequence of real numbers embedded in the DCT coefficient of each segment of the host image.

Blossom Kaur [9], proposes a DCT based scheme in their proposed work. They embedded the watermark in the mid frequency based on the DCT blocks. The watermark is inserted by adjusting the DCT coefficients of the image and the private key. Same private key has been used for image extraction without restoring the original image.

Hsu and Wu [10] proposed a DCT based watermarking technique. They embed the watermark with visually recognizable patterns into the image by selectively modifying the middle-frequency bands of the image. Their embedding technique can survive against cropping, image enhancement and the JPEG lossy compression.

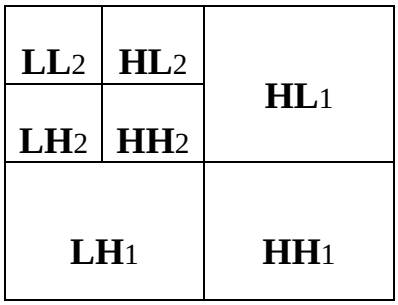
Shinfeng D. Ling [13] proposed a DCT based technique, where they adjust the DCT low frequency coefficients by the concept of mathematical remainder instead of directly replacing the low-frequency components with watermark. This technique will preserve the acceptable visual quality for watermarking image.

A Pavi [11] proposed a DCT based watermarking method operates in the frequency domain embedding a pseudo-random sequence of real numbers ina selected set of DCT algorithm. The watermark is robust to several signal processing techniques and geometric distortions.

Sartid v. [17] proposes that QR Code (Quick Response Code) is embedded with an invisible watermarking using DCT. DCT is used for encoding process to allow QR Code image to be broken up into different frequency bands using block DCT based method; comparison between mid-bands coefficients then embed with the invisible watermarking information into the middle frequency bands. Reverse embed process from the invisible watermark is used for watermark extraction in the QR Code image. This QR Code image with invisible watermark preserves an information hiding text in the QR Code image.

Discrete Wavelet Transform (DWT)

The fundamental concept of DWT is same as of DCT. Only the transformation process may varies therefore the resulting coefficients are different. Wavelet transform uses wavelet filtering like Haar wavelet filter, Daubechies Orthogonal filters and Daubechies Bi-orthogonal filters to transform the image. These filters decompose the frequency into 4 subbandsi.e LL, LH, HL, and HH as shown in figure.



Two level decomposition using DWT

The wavelet based watermarking algorithm are grounded on their decoder requirements, as Blind Detection or Non – blind Detection. The blind detection doesn't require the original image for detecting the watermarks while non – blind detection require the original image.

DWT based Blind Watermark Detection

HAUN [13] proposed a blind watermark technique based on discrete wavelet transform. They embed a watermark using a grey level image to perform 2-level wavelet transform and modify wavelet coefficients using four different methods according to the differences in wavelet coefficients on different wavelet subbands. This method marginally modifies the wavelet parameters, minimizing image degradation.

Xiaoyi Zhou [24] proposed a SoRS algorithm based on SoW scheme [43], in which the watermark is split into four shares. The 2-level DWT is applied and SVD is performed on the HL/LH subband. In SoRS, all the subbands of 2-level DWT performed on the low subband are selected for embedding watermark. Their experimental result shows that

SoRS has the significant enhancement in perceptibility and the robustness under various types of image processing attacks, even though algorithm is weak against scaling attacks.

Chih Chin Lai [23] proposed a hybrid watermarking technique to satisfy both imperceptibility and robustness requirements. DWT–SVD based technique is used for watermarking; use edge information of an image and apply swarm optimization algorithm to find the proper value of scaling factor which is used to determine the watermark strength.

Cai Yong-Mei [14] proposed blind hybrid audio watermarking scheme based on DWT and SVD. The original audio is divided into block and each block is decomposed on DWT for two degree, then first quarter audio approximate subband coefficients are decomposed on SVD transform, to obtain a diagonal matrix. This diagonal matrix is used for embedding watermark.

SanjanaSinha[15] presented a hybrid technique in video watermarking comprises of DWT and Principal Component Analysis (PCA) SPCA, used for reducing correlation among the wavelet coefficients obtained from wavelet decomposition of each video frame there by dispersing the watermark bit into the uncorrelated coefficients. The video frames are first decomposed using DWT and the binary watermark is embedded in the principal components of the low frequency wavelet coefficients.

DWT based Non Blind Watermark Detection

Samira Lagzian [16] proposed a non-blind image watermarking scheme based on redundant DWT (RDWT) and single value decomposition (SVD). First RDWT is applied to both cover and watermark images, then SVD is applied to the LL subbands, after which singular values of the cover image using singular values of the visual watermark is modified.

Tao and Eskicioglu [44] proposed an optimal wavelet based watermarking technique. They embedd binary logo watermark in all the four bands. But they embed the watermarks with variable scaling factor in different bands. The scaling factor is high for the LL subband. Similarity ratio measurement for objective calculation is used to determine the quality of the extracted watermark [19].

IV. Impact of Genetic Algorithm

Genetic Algorithm GAs is an adaptive methods which may be used to solve search and optimization problems. The canonic principles of GAs were first laid down by Holland [41]. The concept of GAs is to make the technique more robust.

Genetic Algorithms are guided by analogy of natural behavior. They exploit with a population of "individuals", each representing a possible solution. The majority conferred individuals are given opportunities to "reproduce", by "cross breeding" with other individuals in the population. The new generation thus produced contains mellower proportion of the characteristics owned by the good members of former generations. The well projected GA will converge to optimal solution of the problem.

Basic Principles

Initially, a coding is formulated for the execution of the Genetic Algorithm over a defined problem. The figure of merit is assigned by "Fitness Function". The parents are selected for reproduction and recombined to generate offspring. These faces are expressed below.

1. **Coding: -**A possible solution is defined as a set of parameters for a defined problem. These parameters "genes" are coupled to form a string of value "chromosome". In genetic terms, these chromosomes are referred to as "genotype" and the information required for the formation of an organism is referred to as the "phenotype".
2. **Fitness Function: -** For the solution of each problem a "Fitness Function" is fabricated. The fitness function retort a single numerical "fitness" or "figure of merit", which is assumed to be commensurable to the "utility" or "ability" of the expression which that chromosome represents.
3. **Reproduction:** - In the facet of GA, particulars are selected from the population and recombined, to produce offspring which will comprise the next generation. A scheme based on favoring the more fit individuals is used for the random selection of the parents from the population.

The mechanism of crossover and mutation is applied for the recombination of the chromosomes of the two selected parents.
The most basic forms of these operations are as follows:

Crossover: The chromosome strings of two individuals are cut at some randomly chosen position producing two "head" segments, and two "tail" segments. A random choice is made to apply crossover on the individuals. Crossover is applied where likelihood is typically between 0.6 and 1.0.

Mutation: After the crossover, mutation is individually applied to each child. It randomly revamps each gene with a small probability (typically 0.001).

4. **Convergence:** -Convergence is the progression towards increasing uniformity. A gene is said to be converged when 95% of the population share the same value [42]. If all the genes have converged then the population is said to be converged.

V. Conclusion

To ensure the robustness of the digital multimedia is the ultimate goal of watermarking system. Various techniques from different domains suggested by different authors are discussed in this paper. All the watermarking schemes have their own advantages, and disadvantages, and each technique is completely different from the other.
From our survey we have found that DWT based scheme provides more robustness to digital multimedia than other proposed schemes. Implementation of Genetic Algorithm improves the quality of watermarked images. Watermark embedded using Genetic Algorithm provides a systematic way to consider the improvements of the Fitness Functions. Hence we have concluded that if Genetic Algorithm is being applied in the digital watermarking, the image becomes more robust and the watermarked quality is also improved.

Acknowledgments

Vagesh Porwal and Siddharth Gupta thanks **Mr. S.P.S.Chauhan**, Assistant Professor, Department of Computer Science & Engineering, Galgotias University for his constant support and guidance throughout the course of whole survey.

References

[1] Navas, K. A., Mathews Cheriyan Ajay, M. Lekshmi, Tampy S. Archana, and M. Sasikumar. "DWT-DCT-SVD based watermarking." In *Communication Systems Software and Middleware and Workshops, 2008.COMSWARE 2008. 3rd International Conference on*, pp. 271-274. IEEE, 2008.

[2] Bhatnagar, Gaurav, and Balasubramanian Raman. "Dual watermarking scheme via sub-sampling in WPT-SVD domain."In *Emerging Trends in Engineering and Technology, 2008.ICETET'08. First International Conference on*, pp. 850-855. IEEE, 2008.

[3] Bedi, S. S., Ashwani Kumar, and PiyushKapoor. "Robust secure SVD based DCT–DWT oriented watermarking technique for image authentication." In*International Conference on IT to celebrate S. Charmonman's 72nd birthday*, pp. 46-1. 2009.

[4] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques."In *Industrial Informatics, 2005.INDIN'05. 2005 3rd IEEE International Conference on*, pp. 709-716. IEEE, 2005.

[5] Shih, Frank Y., and Scott YT Wu. "Combinational image watermarking in the spatial and frequency domains." *Pattern Recognition* 36, no. 4 (2003): 969-975.

[6] El-Gayyar, Mahmoud. "Watermarking techniques spatial domain digital rights seminar." *Germany, May* (2006).

[7] Ruanaidh, J. J. K. O., W. J. Dowling, and F. M. Boland. "Phase watermarking of digital images." In *Image Processing, 1996.Proceedings, International Conference on*, vol. 3, pp. 239-242. IEEE, 1996.

[8] Agrawal, MrsDeepati, MrVikas Gupta, and MrGaurav Mehta. "Digital Watermarking Technique using Discrete Cosine Transform." *IJEIR* 2, no. 1 (2013): 9-14.

[9] Kaur, Blossom, AmandeepKaur, and Jasdeep Singh. "Steganographic approach for hiding image in DCT domain." *International Journal of Advances in Engineering & Technology* 1, no. 3 (2011): 72-78.

[10] Hsu, Chiou-Ting, and Ja-Ling Wu. "Hidden digital watermarks in images."*Image Processing, IEEE Transactions on* 8, no. 1 (1999): 58-68.

[11] Piva, Alessandro, Mauro Barni, Franco Bartolini, and Vito Cappellini. "DCT-based watermark recovering without resorting to the uncorrupted original image."In *Image Processing, 1997.Proceedings, International Conference on*, vol. 1, pp. 520-523. IEEE, 1997.

[12] Feng, Liu Ping, Liang Bin Zheng, and Peng Cao. "A DWT-DCT based blind watermarking algorithm for copyright protection." In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, vol. 7, pp. 455-458. IEEE, 2010.

[13] Huang, Wen-Tzeng, Sun-Yen Tan, Yuan-Jen Chang, and Chin-Hsing Chen. "Robust watermarking techniques for copyright protection using discrete wavelet transform." *WSEAS Trans. Computers* 9, no. 5 (2010): 485-495.

[14] Cai, Yong-mei, Wen-qiangGuo, and Hai-yang Ding. "An Audio Blind Watermarking Scheme Based on DWT-SVD." *Journal of Software* 8, no. 7 (2013): 1801-1808.

[15]Sinha, Sanjana, PrajnatBardhan, SwarnaliPramanick, AnkulJagatramka, Dipak K. Kole, and ArunaChakraborty. "Digital video watermarking using discrete wavelet transform and principal component analysis." *International Journal of Wisdom Based Computing* 1, no. 2 (2011): 7-12.

[16] Lagzian, Samira, Mohsen Soryani, and MahmoodFathy. "A new robust watermarking scheme based on RDWT-SVD." *International Journal of Intelligent Information Processing* 2, no. 1 (2011): 22-29.

[17] Vongpradhip, Sartid, and SuppatRungraungsilp. "QR code using invisible watermarking in frequency domain." In *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2011 9th International Conference on*, pp. 47-52. IEEE, 2012.

[18] Beasley, David, R. R. Martin, and D. R. Bull. "An overview of genetic algorithms: Part 1. Fundamentals." *University computing* 15 (1993): 58-58.

[19] Raphael, A. Joseph, and V. Sundaram. cryptography and Steganography- A Survey." *International Journal of Computer Technology and Applications* 2, no. 3 (2011).

[20] Sadek, Rowayda A. "SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges." *arXiv preprint arXiv: 1211.7102*(2012).

[21] Megalingam, Rajesh Kannan, MithunMuralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian, and VineethSarmaVenugopalaSarma. "Performance comparison of novel, robust spatial domain digital image watermarking with the conventional frequency domain watermarking techniques."In *Signal Acquisition and Processing, 2010.ICSAP'10. International Conference on*, pp. 349-353. IEEE, 2010.

[22] Dubolia, Rakhi, Roop Singh, Sarita Singh Bhadoria, and Rekha Gupta. "Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on PSNR." In *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, pp. 593-596. IEEE, 2011.

[23] Lai, Chih-Chin, Chi-Feng Chan, Chen-SenOuyang, and Hui-Fen Chiang. "A Robust Feature-Based Image Watermarking Scheme." In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2013 14th ACIS International Conference on*, pp. 581-585. IEEE, 2013.

[24] Zhou, Xiaoyi, and Lingfei Wang. "SoRS: An effective SVD-DWT watermarking algorithm with SVD on the revised singular value." In *Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference on*, pp. 1001-1006. IEEE, 2014.

[25]Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, "AnEncrypto-Stego Technique Based secure data Transmission System", PEC, Chandigarh.

[26] B BZaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010.

[27] R. Wolfgang, E. Delp, A watermarking technique for digital imagery: further studies, International Conference on Imaging Science, Systems and Technology, Los Vegas, Nevada, Juillet
1997.

[28] I. Pitas, T. Kaskalis, Applying signatures on digital images, Workshop on Nonlinear Signal and Image Processing, IEEE, NeosMarmaras, June 1995, pp. 460–463.

[29] G. Caronni, Assuring ownership rights for digital images, Proceedings of Reliable IT Systems, VIS'95, Viewveg Publishing Company, Germany, 1995.

[30] K.E. Zhao J., Embedding robust labels into images forcopyright protection, Technical Report, Fraunhofer Institutefor Computer Graphics, Darmatadt, Germany, 1994.

[32] I. Cox, J. Kilian, T. Leighton, T. Shamoon, Securespread spectrum watermarking for images audio and video,Proceedings of the 1996 IEEE International Conference onImage Processing (ICIP'96), Lausanne, Switzerland, Vol. III,pp. 243–246.

[33] I. Cox, J. Killian, T. Leighton, T. Shamoon, Secure spreadspectrum watermarking for multimedia, IEEE Trans. ImageProcess. 6 (12) (1997) 1673–1687.

[34] P. Bas, J.-M.Chassery, B. Macq, Image watermarking: anevolution to content based approaches Pattern Recognition 35(2002) 545–561.

[35] C.-T. Hsu, J.-L.Wu, Hidden signature in images, IEEE Trans.Image Process. 8 (1999) 58–68.

[36] Stefan Katzenbeisser and Fabien A. P.etitcolas, "I*nformation Hiding Techniques for Steganography and Digital Watermarking*," Artech house, Computer security series, pp.15-23, 97-109, 2000.

[37] Neil F.Johnson, ZoranDuric and SushilJajodia, "*Information Hiding, Steganography and Watermarking-Attacks and Counter Measures*," Kluwer academic publisher, pp. 15-29, 2003.

[38] Navas. K A, Sreevidya S, Sasikumar M "A *benchmark for medical image watermarking*", 14th International workshop on systems, signals & image processing and 6th EURASIP Conference focused on speech & image Processing, Multimedia Communication and services IWSSIP-2007 & EC-SIPMCS-2007, Maribor, Slovenia, 27-30 June 2007, pp 249-252.

[39] Alexander Sverdlov, Scott Dexter, AhmetM.Eskicioglu "*Robust SVD DCT based watermarking for copyright protection*",IEEE

Transactions on Image Processing, 10(5), May 2001, pp. 724-735.

[40] S. P. Mohanty, K. R. Ramakrishnan and M. Kankanhalli,"A Dual Watermarking Technique for Images,"*Proceedings of the seventh ACM international conferenceon Multimedia*, Orlando, Florida, USA, 1999, pp.49-51.

[41] J.H. Holland. Adaptation in Natural and Arti_cial Systems.MIT Press, 1975.

[42] K. DeJong. The Analysis and behaviour of a Class of Genetic Adaptive Systems.PhD thesis, University of Michigan, 1975.

[43] X. Zhou, J. Ma and W. Du. SoW: A Hybrid DWT-SVD based SecuredImage Watermarking. In SNS & PCS, 2013, pages 197 – 200

[44] Tao, Peining, and Ahmet M. Eskicioglu. "A robust multiple watermarking scheme in the discrete wavelet transform domain." In *Optics East*, pp. 133-144.International Society for Optics and Photonics, 2004.

First Author Vagesh Porwal has done BCA from IGNOU, Raebareli, Uttar Pradesh, India in 2011 and M.Sc from MDU, Rohtak, Haryana, India in 2013. He is currently pursuing M.tech in CSE from Galgotias University, Greater Noida, Uttar Pradesh, India. Presently he is working of the project "Improving the Robustness of the Digital Watermark using Frequency Domain ".

Second Author Siddarth Gupta has done B.tech in CSE from UPTU, Lucknow, Uttar Pradesh, India in 2012. Currently he is pursuing M.tech in CSE from Galgotias University, Greater Noida, Uttar Pradesh, India.

